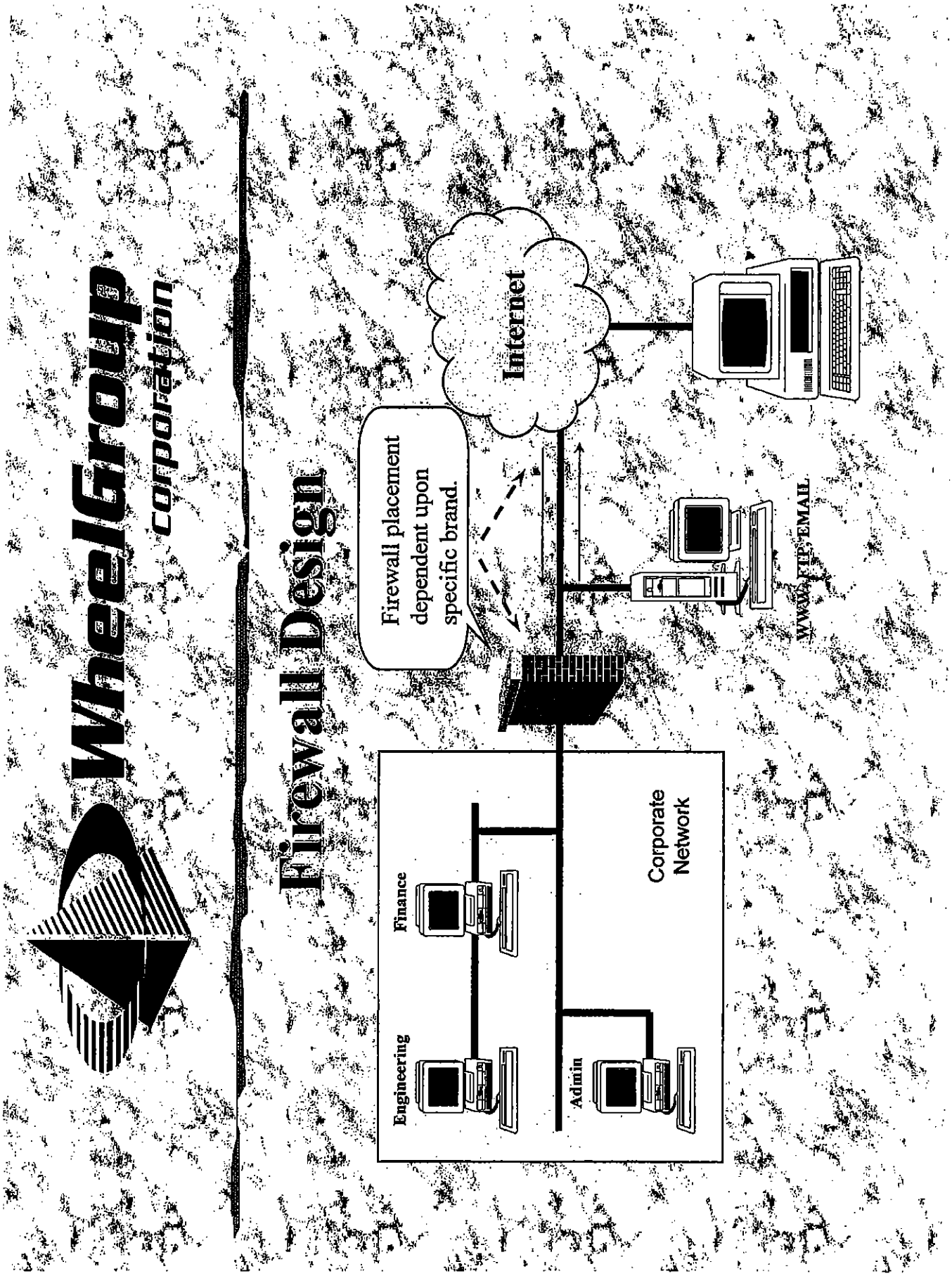
WheelGroup
Corporation
Firewall Design
Firewall placement dependent upon specific brand.
Internet
WWW, FTP, EMAIL
Finance
Engineering
Admin
Corporate Network

Application Gateways

- Provide address translation
- Independent application proxies
- Reduce visible network to a few hosts
  - Firewall server, DNS, WWW, Mail
- Good authentication mechanisms on some firewalls
- No direct connections to internal hosts

Application Gateway Drawbacks

- No real intrusion detection
- Performance problems
- Can't see if alternate routes exist to internal network
- Must be properly configured and constantly maintained
- No security checks on allowed services
- Does not protect external servers - WWW, mail, etc.

Filtering Router

- Block traffic at external router
- Filters on network protocols and applications
- Protects all internal hosts
- Higher performance
- Restrict incoming traffic to specific hosts (WWW,DNS,FTP,Mail)
- Seamless outgoing traffic

Filtering Router Problems

- No intrusion detection
- Must be properly configured and maintained
- No address translation capabilities
- Greater visibility into internal networks
- No security checks on allowed services

WheelGroup
corporation
Finance
Engineering
Admin
Virtual Private Network
Internet
External
untrusted hosts
Finance
Engineering
Admin
Protect your data which flows over untrusted networks

Encryption Techniques

- Public / private key technology
  - Public key distributed to everyone who needs it
  - Private key owned only by single user or host
  - RSA most common
- Private key technology
  - Requires both sides to use the same key
  - Key must be protected
  - DES most common

Encryption Drawbacks

- Doesn't protect your networks - only the data between two protected networks
- Key management can be a problem
- High cost and administrative overhead for application and host based encryption
- False sense of security
- Is the information protected once it arrives

Next Generation Security

- Managed network security
- Intrusion detection
- Monitoring
- Intrusion control and recovery
- Automatic updates of network security system
- Remote control of integrated security systems

WheelGroup
corporation
Intrusion Detection
Internet
External
untrusted hosts
WWW, FTP, EMAIL
Finance
Engineering
Admin
Corporate
Network
Constant vigilance watching incoming and outgoing
network traffic performed by intelligent software

Intrusion Detection Concepts

- Context based intrusion detection
  - Policy violations
  - Activity patterns
    - Hacking tools
    - Ping sweeps
    - Port sweeps
- Content based intrusion detection - Pattern matching

Monitoring

- Personnel dedicated to watching computer networks
  - Security events
  - Availability events
- Computer systems in place to aid monitoring process
  - Trouble tickets
  - Trend analysis
  - Report generation

Intrusion Control and Recovery

- Control intrusion events as they occur
  - Fishbowl a hacker
  - Forensic analysis
  - Track hacker and coordinate with law enforcement
- Recover from a hacking event
  - Find compromised systems
  - Recover crashed systems
  - Prevent future events of a similar nature

Conclusion

- We Provide Security Expertise and Continuity
- NetRanger-Based on Next Generation Security
- Security = Protection + Detection + Response